

IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method to manage secure communications, comprising:
establishing a secure session on a secure site with an external client that communicates from an insecure site;
detecting access attempts during the session directed to insecure transactions, the insecure transactions identified as links to a site that is external to and not controlled by the secure site;
and
transparently managing the access attempts by pre-acquiring content ~~and metadata~~ from the site not controlled by and external to the secure site by accessing the links on behalf of the external client to pre-acquire the content ~~and the metadata~~ and by scanning the content ~~and metadata~~ before determining whether the content ~~and metadata~~ should be made available to the external client during the secure session.
2. (Original) The method of claim 1 wherein the detecting further includes translating non-secure links into secure links for the insecure transactions before presenting results of the access attempts to the external client.
- 3-5. (Cancelled).
6. (Previously Presented) The method of claim 1 wherein managing at least one or more of:
permitting normally occurring security warnings to present messages to the external client by taking no action;
removing the external reference links from a browser page that originally included the reference links before presenting the browser page to the external client, thereby preventing external client access to the external reference links;
generating for and displaying to a custom warning message that is presented to the external client;

issuing alerts, notifications, or advisories to a monitoring entity or log; and
determining the external reference links are low-risk to or trusted by the secure site and
thereby suppressing normally occurring security warnings from being presented to the external
client.

7. (Cancelled).

8. (Currently Amended) A method to manage secure communications, comprising:
detecting insecure transactions occurring during a secure session, wherein the insecure
transactions result from actions requested by an external client participating in the secure
session;

inspecting the insecure transactions in advance of satisfying the actions requested by pre-
acquiring content ~~and metadata~~ associated with the insecure transactions before making available
to the external client, and wherein the insecure transactions are associated with links to an
external site, and wherein content ~~and metadata~~ are pre-acquired from the external site via the
links and scanned on behalf of the external client; and

making a determination in response to the inspection for at least one of the following:
permitting the insecure transactions to proceed unmodified by performing the actions requested
for the external client, permitting the insecure transactions to proceed in a modified fashion, and
denying the insecure transactions by denying the actions requested.

9. (Cancelled).

10. (Currently Amended) The method of claim 8, ~~claim 9~~ wherein the making a
determination further includes, permitting the insecure transactions to proceed in the modified
fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links
to HTTP over Secure Sockets Layer (HTTPS) in order to suppress the security warning
messages.

11. (Cancelled).

12. (Previously Presented) The method of claim 8 wherein the making a determination further includes permitting the insecure transactions to proceed unmodified by permitting normally occurring security warnings to be presented to the external client before satisfying the external client access attempt to reference the external site.
13. (Previously Presented) The method of claim 8 wherein the making a determination further includes permitting the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within a proxy making the external client access attempt appear to be part of the secure session.
14. (Previously Presented) The method of claim 8 wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of the denial.
15. (Previously Presented) The method of claim 8 wherein the making a determination further includes denying the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt.
16. (Currently Amended) A secure communications management system, comprising:
a secure communications manager processing on a machine associated with a secure site and which manages a secure session with an external client that is associated with an insecure site; and
a proxy that processes on the machine within the secure site and which interacts with the secure communications manager in order to inspect insecure communications requested by the external client during the secure session by pre-acquiring content and ~~metadata~~ associated with the insecure communication before making available the content and ~~metadata~~ accessible to the external client, and wherein the proxy selectively processes the insecure communications on behalf of the external client within the secure session, and wherein the content and ~~metadata~~ are acquired from an external site not associated with the secure site and the external client and the

content and metadata are scanned to determine whether to make the content and metadata accessible to the external client.

17. (Original) The secure communications management system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session.

18. (Previously Presented) The secure communications management system of claim 16 wherein the proxy selectively modifies a number of the insecure communications and permits them to proceed thereby suppressing normally occurring security warning messages that the secure communications manager issues.

19. (Previously Presented) The secure communications management system of claim 16 wherein the proxy selectively leaves a number of the insecure communications unchanged and permits secure communications manager to issue security warning messages to the external client.

20. (Previously Presented) The secure communications management system of claim 16 wherein the proxy selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records the denial in a log.

21. (Previously Presented) The secure communications management system of claim 16, wherein the proxy selectively issues custom warning messages or explanations to the external client regarding a number of the insecure communications.

Claims 22-30. (Cancelled)